IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC., a California Corporation, Plaintiff and Counterclaim-Defendant, v. INTERNET SECURITY SYSTEMS, INC., a Delaware corporation, INTERNET SECURITY SYSTEMS, INC., a Georgia corporation, and SYMANTEC CORPORATION, a Delaware corporation, Defendants and Counterclaim-Plaintiffs.	C. A. No. 04-1199 (SLR)

SRI'S RESPONSE TO JOINT OPENING CLAIM CONSTRUCTION BRIEF OF ISS AND SYMANTEC

Dated: June 30, 2006

FISH & RICHARDSON P.C.

John F. Horvath (#4557)
FISH & RICHARDSON P.C.
919 N. Market St., Ste. 1100
P.O. Box 1114
Wilmington, DE 19889-1114
Telephone: (302) 652-5070
Facsimile: (302) 652-0607

Howard G. Pollack (CA Bar No. 162897)
Katherine D. Prescott (CA Bar No. 215496)
FISH & RICHARDSON P.C.
500 Arguello St., Ste. 500
Redwood City, CA 94063
Telephone: (650) 839-5070
Facsimile: (650) 839-5071

Attorneys for Plaintiff/Counterclaim Defendant
SRI INTERNATIONAL, INC.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

PAGE

STATUTES

I. INTRODUCTION

On June 9, 2006, ISS and Symantec (collectively, "the Defendants") submitted their Joint Opening Claim Construction Brief (the "Joint Brief"). In doing so, the Defendants have made the strategic choice to join forces, now arguing for proposed constructions of claim terms as to which they had previously, and often sharply, disagreed. Notably, the constructions now proposed in the Defendants' joint brief are a hodgepodge of some previously proposed only by ISS, others previously proposed only by Symantec, and hybrid constructions that either combine elements of both the Defendants' earlier constructions or include elements that are entirely novel. In many cases, the Defendants have simply abandoned the material differences between their original constructions, even though throughout this case, and in particular through their expert reports and in all of their depositions, they adamantly maintained those distinctions.

The reason for the Defendants' sudden shift is apparent. It is certainly not, as the Defendants say, to reduce the issues before the Court — the Defendants continue to seek construction of terms that have plain English-language meanings, or are not relevant to any issue in dispute and for which, therefore, construction is unnecessary. *U.S. Surgical Corp. v. Ethicon, Inc.*, 103 F.3d 1554, 1568 (Fed. Cir. 1997). Rather, the Defendants are just picking and choosing constructions they currently believe best support their latest non-infringement and invalidity positions, while at the same time trying to mask the fundamental weakness of these positions revealed by their previous inability to agree.

That the Defendants' claim constructions remain unprincipled is seen most clearly in their wholesale resort to the details of the specification of the patents-in-suit, and their virtual disregard of the language of the claims themselves. But claim construction begins with the language of the claims. *Innova/Pure Water, Inc., v. Safari Water Filtration Sys. Inc.*, 381 F.3d 1111, 1116 (Fed. Cir. 2004). Once focused on the specification, the Defendants then attempt to import limitations from preferred embodiments into almost

every claim term for which they propose a construction. It is well-established, however, that such constructions are impermissible. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1316 (Fed. Cir. 2005). Specific examples of the ways in which the Defendants improperly and selectively import some, but not all, of the limitations from the described embodiments into the claims are discussed more fully below.

The Defendants seem to suggest that the rule prohibiting importation of limitations of preferred embodiments into claims is a flexible rule, often departed from, citing *Inpro II Licensing v. T-Mobile USA Inc.* for the proposition that "claims [do not] enlarge what is patented beyond what the inventor has described as the invention." 2006 WL 1277815 (Fed Cir. 2006) (quoting *Network, LLC v. Central Corp.*, 242 F.3d 1347, 1352 (Fed. Cir. 2001)). But the case law the Defendants cite demonstrates that departure is permitted only when the specification itself or arguments made during prosecution make clear that such limitations were intended by the patentee.[1]

Here, the specification of the patents-in-suit describes preferred embodiments of various claimed features without stressing the importance of those features to the invention and without disparaging other possibilities. Likewise, no arguments were made during prosecution distinguishing prior art on the basis of the presence or absence of any claimed feature. In short, the factors that warranted importation of limitations of a preferred embodiment into claim terms in the cases the Defendants cite are completely

[1] The District Court in *Inpro II* construed a broad claim term, "host interface," to mean more narrowly "a direct parallel bus interface," which was described in a preferred embodiment in the specification of the patent-in-suit. Critical to the District Court's narrow construction were statements in the specification itself describing the direct parallel bus interface as a "very important feature" of the invention and disparaging other types of interfaces, (2006 WL 1277815, at *3-4), and statements made during prosecution of the patent distinguishing the invention over prior art as having a direct, rather than a serial, interface. *Id.* at *5. Similarly, in *Network*, which the Defendants also cite, the District Court's construction of a claim term as having limitations found in a preferred embodiment was affirmed as justified in light of statements made during the prosecution of the patent-in-suit. 242 F.3d at 1353.

absent here, and the well-established principle prohibiting such constructions is fully applicable.

The Defendants also attempt to justify their disregard of the claim language and of the prohibition on reading limitations of preferred embodiments into claims by contending that they are merely applying "definitions" of terms that the specification, acting as its own lexicon, provides. But this is decidedly not a definition case — the specification of the patents-in-suit provides no definitions of any kind. The Defendants attempt to characterize *examples* found in the specification as *definitions*, but to no avail. It is well-established that a specification must be explicit in defining terms in order to act as its own lexicon. *Rexnord Corp. v. Laitram Corp.*, 274 F.3d 1336, 1342 (Fed. Cir. 2001) ("patent law permits the patentee to choose to be his or her own lexicographer by *clearly setting forth an explicit definition* for a claim term") (emphasis added). Here, the specification provides no explicit definitions and expresses no intent to do so.

Finally, realizing the lack of support for their constructions in the intrinsic evidence, and despite the Defendants' numerous citations to *Philips* for the evils of undue reliance on extrinsic evidence, the Defendants are forced to rely heavily on extrinsic evidence to support their proposed constructions. But the Defendants select their extrinsic evidence with care: they do not rely on any evidence from any Symantec expert. Given that most of the jointly-proposed claim constructions were formerly ISS's proposals, and given the numerous conflicts between the parties' respective experts, the Defendants now apparently want to distance themselves from positions that Symantec has formerly taken.

In comparison to the Defendants' approach of selectively importing limitations from the specification with no justification, SRI has focused on intrinsic rather than extrinsic evidence. Thus, the constructions advanced by SRI are based first and foremost on the language and context of the claims, as the Federal Circuit on numerous occasions has indicated is the required approach. Unlike the Defendants, SRI has refrained from

impermissibly importing limitations from preferred embodiments found in the specification. Because SRI's approach is consistent with the principles of claim construction adopted and required by the Federal Circuit, SRI's proposed claim constructions should be adopted.

II. ARGUMENT

In its Opening Claim Construction Brief, ("Opening Brief") (D.I. 265) SRI set forth proposed constructions for six disputed claim terms. SRI also addressed several terms for which it believed claim construction was unnecessary but, responding to the Defendants' inclusion of them in the Joint Claim Construction Statement, proposed constructions for use in the event that the Court found that construction would be helpful. The Defendants, in their Joint Brief (D.I. 267), failed to address one term all the parties originally contended requires construction — "responding . . ." / "invoking countermeasures" — apparently because the Defendants no longer dispute SRI's proposed construction.[2] The Defendants also failed to address four terms the Defendants insisted on including in the proposed construction statement, over SRI's objection: 1) "peer-to-peer;" 2) "selected from;" 3) "signature matching detection method;" and 4) "proxy server." Despite the position taken during the process of preparing the Joint Claim Construction Statement, the Defendants apparently now prefer that the Court not construe these terms – even though they have expressly relied on their interpretation of "signature matching detection method," as well as "API" (a term never even identified in

[2] SRI requests the Court to adopt its proposed construction for these terms as set out and explained in SRI's Opening Claim Construction Brief

the Joint Claim Construction Statement), to argue non-infringement.[3] SRI's response to the Defendants' various proposals is set forth in detail below.

A. Hierarchical Architecture

1. Monitor / Network Monitor

Claim Term	**"monitor" / "network monitor"**
SRI Construction	process or component in a network that can analyze data; depending on the context in specific claims, the network monitor may analyze network traffic data, reports of suspicious network activity or both. Service monitors, domain monitors and enterprise monitors are examples of network monitors
Defendants' Joint Construction	generic code that can be dynamically configured and reconfigured with reusable modules that define the monitor's inputs, analysis engines and their configurations, response policies and output distribution for its reports

SRI's proposed construction of "monitor" and "network monitor" is consistent with the plain and ordinary meaning of those terms. Contrary to the Defendants' arguments, the inventors did not use the specification to define the terms "monitor" or "network monitor," or to give them a special meaning. Instead, the inventors used them in a generic way in both the specification and the claims, and used the additional language of the claims to more specifically delineate the required attributes of each of the claimed monitors. For example, the "network monitors" of claim 1 of the '203 patent "detect [] suspicious network activity based on analysis of network traffic data selected from the" categories listed in the Markush grouping, and then generate "reports of said suspicious activity." In claim 1 of the '212 patent, the claimed network monitors detect suspicious network activity "based on an analysis of network traffic data, wherein at least one of the network monitors utilizes a statistical detection method." Thus, while the terminology "network monitor" standing alone may be somewhat broad and generic, the

[3] SRI briefly reiterates its positions on "signature matching detection method" and "API" below. SRI believes the other terms ("peer-to-peer," "selected from" and "proxy server") need not be construed.

term does not stand alone in the claims, which themselves provide the necessary context to adequately define the network monitors through a description of their function.

By contrast, the Defendants' proposed construction improperly attempts to read several carefully selected limitations from the preferred embodiment — for example, that the network monitor be "dynamically configurable" — into the claims. The Defendants argue they are entitled to limit the claims to the preferred embodiment that is described in the specification because the terms "monitor" and "network monitor" lacked meaning to those of skill in the art at the time the application was filed, and that as a result, the inventors had to define these terms in the specification. But the Defendants are wrong on both counts.

The Defendants seek to avoid the well-established rule requiring that a specification explicitly define terms in order to serve as its own lexicon. Citing to *Irdeto Access, Inc. v. Echostar Satellite Corp.* for the proposition that "even when guidance is not provided in explicit definitional format, the specification may define claim terms by implication such that the meaning may be found in or ascertained by a reading of the patent documents" (383 F.3d 1295, 1300 (Fed. Cir. 2004)), the Defendants suggest that terms allegedly having no meaning to those of ordinary skill in the art are necessarily defined by the specification.

First, even a cursory review of the numerous prior art references the Defendants have cited in support of their invalidity contentions shows that the terms "monitor" and "network monitor" were widely known and used in the intrusion detection field since at least the early 1990s to broadly describe all manner of processes and components that looked at data. [*See e.g.,* Ex. B (DIDS Feb. 1991)[4]; Ex. C (DIDS Oct. 1991); Ex. D (NSM); Ex. E (ISM)]. In fact, two of the references the Defendants rely upon in their

[4] Unless otherwise noted, all referenced exhibits are attached to the Declaration of Kyle Wagner Compton in support of SRI's Reply to Joint Opening Claim Construction Brief of ISS and Symantec.

invalidity contentions contain the word "monitor" in their title, namely, the Network Security Monitor or NSM paper, and the Internet Security Monitor or ISM paper. [Exs. D, E (NSM and ISM)]. The use of the term "monitor" in all of these references, which were published in the early 1990s, clearly shows that use of the generic term "monitor" was well known to those of skill in the art of intrusion detection.

Moreover, in *Irdeto*, importation of limitations of a preferred embodiment into the claims was premised on facts not present here. The *Irdeto* Court makes clear that definition by implication was appropriate because the patentee, in order to overcome an obviousness rejection of all claims during prosecution of the patent-in-suit, "informed the examiner and all competitors that the [construed claim terms] have no accepted meaning in the art and 'are very adequately described in the specification,'" concluding that "[t]he applicant's use of those terms in the specification thus controls their scope." 383 F.3d at 1300. SRI made no arguments concerning the meaning of "monitor" or "network monitor" during the prosecution of the patents-in-suit, and never stated or suggested during prosecution that the meaning of such claim terms was laid out in the specification.

Also, contrary to the Defendants' arguments, the specification neither expressly nor implicitly defines the terms "monitor" or "network monitor." While it is generally true that a patentee may use the specification to define the meaning of a word that is used in a claim, "any special definition given to [the] word must be *clearly* defined in the specification. The written description part of the specification itself does not delimit the right to exclude." *Markman v. Westview Instr., Inc.*, 52 F.3d 967, 980 (Fed. Cir. 1995) (emphasis added; internal citations omitted). Instead, the terms of a claim are "generally given their ordinary and customary meaning," and are construed to have a special meaning only when "the special definition of the term is *clearly* stated in the patent specification or file history." *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996) (emphasis added).

Not only does the specification fail to define "monitor" or "network monitor", but the Defendants selectively, and inexplicably, import only *some* of the characteristics of the monitors described in the preferred embodiment. For example, the Defendants would like a construction requiring the use of "generic code" that is "dynamically configured and reconfigured" and has "reusable modules" that define several more alleged required characteristics. Yet the Defendants' construction stops short of drawing in all the details of the specification, for example, that the monitor have both a "statistical anomaly detection unit" and a "signature-based inference unit" or that the monitor employ specific statistical detection methods or invoke particular responses. With respect to dynamic configuration in particular, the specification teaches that this feature is only one of "five categories of interoperation" for monitors. Why are the other four features not likewise required? The Defendants do not say, but it is obvious the Defendants cannot credibly import all of these limitations. However, they have no basis for selectively importing the limitations they do recite in their proposed construction, other than their belief that the ones they picked are sufficient to avoid liability for infringement.

Of their several proposed limitations, the Defendants only attempt to justify the importation of one — "reusable software architecture" — characterizing language from the specification that suggests some advantages of reusable software as warranting disavowal of any construction that does not require reusable software. Specifically, the Defendants cite *On Demand Machine Corp. v. Ingram Indus., Inc.* for the proposition that "when the scope of the invention is clearly stated in the specification, and is described as the advantage and distinction of the invention, it is not necessary to disavow explicitly a different scope." 442 F.3d 1331, 1340 (Fed. Cir. 2006).

As an initial matter, the supposed statements of advantage that the Defendants cite are largely contrived. The specification contains only a single reference to "reusable software:" "This reusable software architecture can reduce implementation and maintenance efforts." [Ex. A ('338 patent) at 11:7-8]. Other portions of the specification that the Defendants cite make no reference to reusable software — and in fact, do not describe any supposed advantages of reusable software. The other portions of the specification that the Defendants rely on in this context merely describe functions of the disclosed system which the Defendants *characterize* as advantageous.

As to the case law cited, *On Demand Machine* involved a very different set of facts. There, the Court concluded that repeated reference to the narrowness of scope of a feature which is "the focus of the [] patent," and which is distinguished from other alternatives on the basis of that narrowness of scope, amounted to a disavowal of broader scope of that feature. 442 F.3d at 1340. *On Demand Machine* does not stand for the general principle that mere statement of advantages of a feature in the specification amounts to a disavowal of all other features, and indeed, such a rule would essentially *require* that any and all limitations of preferred embodiments — which are, after all, preferred due to perceived advantages that they possess — be imported into the claims. That is not and has never been the law, and the Defendants' attempt to read *On Demand Machine* as supporting such a broad and non-sensical rule simply reaches too far.

Reusable software architecture, referenced only once in the specification, is decidedly not the focus of the patents-in-suit and the vague recitations of advantage that the Defendants have concocted are readily distinguishable from the clear and repeated statements of preference cited in *On Demand Machine*. Indeed, there is no emphasis of

any feature or disparagement of any alternative to any feature in the specification of the patents-in-suit that can reasonably be viewed as a disavowal of scope by SRI.

Consequently, the terms "monitor" and "network monitor," which were known and used generically in the art of intrusion detection, should be construed to have their plain and ordinary meaning as proposed by SRI, and the Court should decline the Defendants' invitation to selectively import limitations from the preferred embodiments into the claims under the guise of "defining" these easily understood terms.

2. Specific Types of Network Monitors

Claim Term	**"hierarchical monitor"**
SRI Construction	a process or component in a network that receives reports from at least one lower-level monitor
Defendants' Joint Construction	a network monitor that receives reports as input from one or more network monitors that are at a lower layer in the analysis hierarchy

Claim Term	**"service monitor"**
SRI Construction	SRI does not believe the term needs construction but, if construed, should be construed to mean a network monitor that analyzes data from individual components or services
Defendants' Joint Construction	a network monitor that provides local real-time analysis of network packets handled by a network entity

Claim Term	**"domain monitor"**
SRI Construction	SRI does not believe the term needs construction but, if construed, should be construed to mean a network monitor that analyzes data from a domain
Defendants' Joint Construction	a network monitor that receives and analyzes intrusion reports disseminated by service monitors

Claim Term	**"enterprise monitor"**
SRI Construction	SRI does not believe the term needs construction but, if construed, should be construed to mean a network monitor that analyzes data from an enterprise, *i.e.* a collection of domains
Defendants' Joint Construction	a network monitor that receives and analyzes intrusion reports disseminated by domain monitors

As with the terms "monitor" and "network monitor," the Defendants try to read into the term "hierarchical monitor" features from a preferred embodiment. In particular,

the Defendants construe the term "hierarchical monitor" to mean a "network monitor" that receives reports from one or more lower-level network monitors in the analysis hierarchy. By recursively defining the "hierarchical monitor" to be a "network monitor," the Defendants import into the "hierarchical monitor" term all the features of the preferred embodiment they improperly attempt to import into the term "network monitor." That is improper for the reasons explained above.

As in the case of "network monitor", the claims point the way to the proper construction. The term "hierarchical monitor" or "hierarchically higher network monitor" would be understood by a person of skill in the art to mean a process or component in a network that receives reports from at least one lower-level monitor, because that is how the context of the remaining language of the claims defines that component. As explained in SRI's Opening Brief at 8-9 and 13-14, the claim language of the independent claims of the hierarchy patents is unmistakable in its differentiation between the "network monitor" and its function and place in the hierarchy, and the "hierarchical monitor" which resides in a different place and performs different functions. If the intent was to define these different monitors as the same thing, the language of the claims would clearly be something other than what it is. Consequently, SRI's construction of "hierarchical monitor" should be adopted.

As with the term "hierarchical monitor," the Defendants attempt to read into the "service monitor," "domain monitor," and "enterprise monitor" terms the same limitations that they want to read into "network monitor." SRI has explained above why that is improper. Moreover, the Defendants try to read into these terms the particular *three-tiered* analysis hierarchy that is described as a preferred analysis hierarchy embodiment in the specification. Thus, the Defendants try to limit "domain monitors" to network monitors that receive and analyze reports only from "service monitors," and try to limit "enterprise monitors" to network monitors that receive and analyze reports only

from "domain monitors."[5] But, as with the characteristics of the preferred network monitor described in the specification, importing all the particular characteristics of the network analysis hierarchy example described in the specification is not intended and should not be used to limit the claims. For example, there is nothing in the description in the specification that would preclude an enterprise monitor from receiving reports directly from a service monitor in a two-tiered, rather than three-tiered, hierarchy. In fact, the dependent claims establish that none of the independent claims can be limited to specifically a three-tiered hierarchy. Dependent claims 12 and 23 of the '212 patent, dependent claims 10 and 21 of the '203 patent, and dependent claims 11, 22, 32, 42, 52, 62, 72, 82 and 92 of the '615 patent all explicitly add the third tier. Accordingly, the Defendants' attempt to limit the terms by importing requirements described in the specification must be rejected.

3. Terms Relating to Deploying an Analysis Hierarchy of Monitors

Claim Term	**"hierarchical event monitoring and analysis"**
SRI Construction	monitoring events through the use of a hierarchical monitor
Defendants' Joint Construction	monitoring and analyzing events through the use of network monitors that are configured to form an analysis hierarchy of two or more layers

Claim Term	**"deploying a plurality of network monitors"**
SRI Construction	SRI does not believe the term needs construction but, if construed, should be construed to mean locating two or more network monitors so as to allow them to receive data to be monitored and/or to send information
Defendants' Joint Construction	installing and configuring two or more network monitors so that together they form an analysis hierarchy defined by the network monitors' inputs and output distribution

The Defendants construe the terms "deploying a plurality of network monitors" and "hierarchical event monitoring and analysis" to include configuring the network monitors to form an analysis hierarchy and analyzing data through the configured

[5] Joint Brief at 20.

analysis hierarchy, respectively. The Defendants include the term "configured" in their proposed constructions to read into this claim language features from the preferred embodiment described in the specification. It is interesting that Symantec in particular now believes that "hierarchical event monitoring and analysis" requires the notion of "configuring", given that its prior position was that the claim term need not be construed.

The first reason to reject the Defendants' construction is, of course, that it has no basis in the claim language, which says nothing about "configuring" or "configuration." Instead, and consistent with their approach on all the disputed terms, the Defendants turn immediately to the specification; there, they rely on the following language:

> [M]onitors ***may include*** different resource objects 32 having different configuration data and methods . . . Customizing and dynamically configuring a monitor 16 thus becomes a question of building and or modifying the resource objects.

[Ex. A at 11:5-12 (emphasis added)]. The cited language does not require that monitors be "configured" at all, let alone configured in the manner the Defendants assert. It simply says monitors *may* include configurable elements, and that configuration is an option. The Defendants' constructions requiring that monitors be configured are therefore not only unsupported by the claims, they are unsupported by the specification. Given this, and given the further problem that importing a vague "configuring" limitation into the claims obscures, rather than clarifies, their meaning, the Defendants' construction must be rejected.[6]

The Defendants disparage SRI's constructions as "divorced from the specification." Resort to the specification is not required to construe these claim terms, however, because their meaning is clear from the context of the claim language itself and

[6] Indeed, given that the Defendants have already tried to import a "dynamically configured" limitation in their asserted definition of "network monitor," importing another "configuration" limitation into the deploying language would make the Defendants' own proposal so confusingly redundant as to leave the jury lost as to what it all is supposed to mean.

the language of other related claims. The construed terms appear in independent claims, and the limitations to which they refer are further refined by a host of dependent claims. For example, "hierarchical event monitoring and analysis", which appears in the *preamble* of claim 1 of the '203 patent, is simply a statement of context and, to the extent it is a limitation at all, the hierarchy described in that claim is progressively further defined by claims 2-11. The "deploying a plurality of network monitors" language, also appearing in claim 1 of the '203 patent, is further limited by claims 6, 7 and 9 where the location and characteristics of the deployment are further refined.[7] Notably, none of the numerous limitations added by the dependent claims themselves even require that monitors be "configured." SRI's proposed constructions are consistent with the scope of the broader independent claims, which are progressively limited by the dependent claims. Thus, these claim terms and their use in the independent claims should not be construed to include limitations found only in the specification.

The Defendants also criticize SRI's proposed constructions as not enabled by the specification.[8] These alleged enablement issues are, in the first instance, not relevant to claim construction. Further, these arguments are raised for the first time in the Joint Brief. Such arguments do not appear in any clear form in the Defendants' validity contentions or expert reports. As explained in more detail below in the discussion of hierarchical analysis, the allegations also simply misunderstand the disclosure of the patents. Accordingly, because they are untimely and because they lack factual support, the Court should decline to credit the Defendants' vague allegations that the claims lack enabling disclosure and should construe the claims as proposed by SRI.

---

[7] The dependent claims of the '615 and '212 patents are to similar effect.

[8] The Defendants cite *On Demand Machine*, 442 F.3d at 1338, in connection with their enablement discussion. That case, and in particular, the cited language, has nothing to do with enablement.

4. Terms Relating to Analysis at the Hierarchical Level

Claim Term	**"automatically receiving and *integrating* the reports of suspicious activity, [by one or more hierarchical monitors]"**
SRI Construction	without user intervention, receiving reports and combining those reports into another functional unit
Defendants' Joint Construction	automatically receiving and combining the reports of detected suspicious network activity

Claim Term	**"wherein integrating comprises *correlating* intrusion reports reflecting underlying commonalities"**
SRI Construction	combining the reports based on underlying commonalities between them
Defendants' Joint Construction	determining relationships among the reports of detected suspicious network activity

The Defendants, noting that the term "integrating" does not appear in the specification of the patents-in-suit, look to the following dictionary definition as support for their proposed construction:[9]

> 1. To bring together or incorporate (parts) into a whole. 2. to make up, combine, or complete or produce a whole or a larger unit, as parts do. 3. to unite or combine.[10]

SRI fully agrees with the Defendants' dictionary definition, which supports SRI's proposed construction and demonstrates that the Defendants' construction is incorrect.

The dictionary definition above indicates that "integrate" means combining pieces together. SRI's proposed construction of "integrating" also requires "combining." The Defendants depart from their own dictionary definition, however, by proposing that "integrate" means only "to combine," and nothing more. That is, they read the definition above to mean:

---

[9] It is ironic that the Defendants disparage SRI's proposed construction for "integrating" as allegedly being unsupported by the specification of the patents-in-suit, while they themselves look solely to a dictionary definition to support their own proposed construction.

[10] Joint Brief at 25.

to ~~make up,~~ combine~~, or complete or produce a whole or a larger unit, as parts do~~

There is no justification for deleting 90% of the dictionary definition that the Defendants have themselves proposed or resorting to the third usage of the word "integrate" while ignoring the first and second usages entirely. SRI's construction is consonant with the scope of the dictionary definitions from both sides, emphasizing that "integrating" means more than only combining — it means combining to produce another unit or "whole."

The Defendants seek to further substantiate their departure from their own dictionary definition by citing deposition testimony from the inventors of the patents-in-suit. Inventor testimony is an improper basis for claim construction.[11] *Arlington Industries, Inc. v. Bridgeport Fittings, Inc.*, 345 F.3d 1318, 1330 (Fed. Cir. 2003) (an inventor's testimony "is of little consequence in the claim construction analysis."); *Markman*, 52 F.3d at 983 (an inventor's testimony on claim construction "is entitled to no deference"). Accordingly, the Court should reject the Defendants' construction, which relies on only one portion of their own proposed dictionary definition, and adopt SRI's construction, which properly reflects the full meaning of the term "integrating."

SRI's proposed meaning of "integrating" is also consistent with the disclosure of the specification, which explains that one of the benefits of integrating reports of suspicious activity into a new functional unit is to allow that new data unit to be further automatically processed by the system, for example, by a peer or at a hierarchically higher level. [*See, e.g.*, Ex. A at 3:66-4:19; 9:64-10:9; 11:41-46 ("analysis results" of monitors are defined in a structure similar to "event records" to allow "hierarchical processing of analysis results as event records by subscriber monitors.")] In other words, the ability to share analysis results in a distributed, potentially multi-level hierarchy is

[11] This is especially true where the inventors, who are not trained in claim construction or legal analysis, were grilled over multiple days and subjected to hour after hour of semantically twisted word play and far-fetched hypothetical questions with the sole goal of creating the sound bites the Defendants now seek to make the cornerstone of their arguments.

one aspect of the inventions that achieves the goals of "scalability" and the ability to automatically recognize more "global" attacks.

With respect to the term "correlating," the Defendants argue that the specification does not describe how correlation is done,[12] and again resort to extrinsic evidence — dictionary definitions and inventor testimony — to support their proposed construction of that term. As with their approach to "integrate," the Defendants cite a dictionary definition but then selectively rely on only a portion of it.[13] The Defendants further argue, particularly based on their allegation of lack of disclosure relating to correlation,[14] that recourse to extrinsic evidence is warranted because correlation was not known to persons having skill in the art in 1998.[15] This argument, however, is directly contrary to their contention that correlation is allegedly taught by the prior art they assert for the purposes of validity.[16]

The Defendants' arguments again simply misunderstand, or intentionally ignore, the teaching of the patent specification as a whole. The Defendants assert that there is "little disclosure" of correlation or "what the hierarchical monitors do" in the

---

[12] Although the Defendants continue to refer to the issue of enablement, as discussed above, their expert reports do not raise lack of enablement of "integrating" or "correlating" as a basis for invalidity.

[13] The Defendants' proposed dictionary definition of "correlate" is: "to place in or bring into mutual or reciprocal relation; establish in orderly connection: *to correlate expenses and income*." The Defendants' proposed construction of "correlating," however, simply extracts the term "relationship" from this definition, and ignores that the relationship must be "mutual or reciprocal." Indeed, the Defendants' proposed construction does not describe the nature of the relationship in any way.

[14] Joint Brief at 14-15.

[15] "Extrinsic evidence . . . may be used to aid a court in construing claim terms as they would be understood in the relevant art." *Goldenberg v. Cytogen, Inc.*, 373 F.3d 1158, 1164 (Fed. Cir. 2004).

[16] Joint Brief at 3. The Defendants also cite, at page 15, the testimony of Frank Jou, the developer of the Ji Nao system, that correlation was an "open question" with regard to that system, yet the Defendants have moved for summary judgment that Ji Nao anticipates the hierarchy claims, including those reciting correlation. This lack of even an attempt at consistency just points out the arbitrary and disingenuous nature of the Defendants' arguments.

specification. Yet, reading the patent as a whole it is clear that, in the preferred embodiment disclosed in the specification, the higher-level monitors perform their analysis on reports of suspicious activity using a similar analytical approach as the lower-level network monitors, only applying a potentially different set of "rules." [*See, e.g.,* Ex. A at 11:33-55 (explaining that the resource object defines the structure of the "event stream", *i.e.* the input to a monitor, as well as the "semantics employed by the analysis engine to process the event stream.")] The specification provides an example of using statistical analysis at the higher level monitor by generating statistical profiles built from "event distribution measures." [Ex. A at 6:34-37 ("event distribution measures are useful in correlative analysis performed by a monitor 16a-16f that receives reports from other monitors 16a-16f.")]. The specification also describes a similar, recursive use of signature analysis at the higher level monitor using different rules (*i.e.* "signature-analysis objects") to perform integration. [Ex A at 7:23-42]. The Defendants quote only a portion of this disclosure and misrepresent it as describing "aggregation." The specification reads:

> As shown, the monitor 16 also includes a signature engine 24. The signature engine 24 maps an event stream against abstract representations of event sequences that are known to indicate undesirable activity. Signature-analysis objectives **depend on which layer in the hierarchical analysis scheme the signature engine operates**. Service monitor 16a-16c signature engines 24 attempt to monitor for attempts to penetrate or interfere with the domain's operation. The signature engine scans the event stream for events that represent attempted exploitations of known attacks against the service, or other activity that stands alone as warranting a response from the monitor. **Above the service layer**, signature engines 24 **scan the aggregate of intrusion reports from service monitors in an attempt to detect more global coordinated attack scenarios** or scenarios that exploit interdependencies among network services. **Layering signature engine analysis** enables the engines 24 to avoid misguided searches along incorrect signature paths in addition to distributing the signature analysis.

[Ex. A at 7:23-42 (emphasis added)]. Thus, the patent specification clearly provides detailed disclosure of different possible mechanisms by which the preferred embodiment's hierarchical monitors perform integration, including, for example, "layering" signature analysis, building statistical profiles of event distribution measures, or both. "This tiered collection and correlation of analysis results allows monitors 16a-16f to represent and profile global malicious or anomalous activity that is not visible locally." [Ex. A at 8:43-46]. SRI's proposed constructions of "integrating" and "correlating" are consistent with this teaching without improperly importing limitations.

One additional flaw in the Defendants' proposed construction of "correlating" is that it ignores that term's dependence upon the term "integrating." Specifically, correlation is claimed as a type of integration, and claims using the term "correlating" are dependent upon claims using the term "integrating." It is well-established that claims that depend from a prior claim incorporate all of the limitations of the prior claim. 35 U.S.C. § 112 ¶ 4; *see also Festo Corp. v. Shoketsu Kinzoku Kogyo Kabushiki Co., Ltd.*, 234 F.3d 558, 590 n.7 (Fed. Cir. 2000) (reversed on other grounds). The Defendants' proposed construction of "correlating" needlessly reiterates that "reports of detected suspicious of network activity" are the object of the correlation step. That is already required by the "integrating" claims, from which the "correlating" claims depend. On the other hand, the Defendants' proposed constructions fail to distinguish between the level of data analysis in the integration step versus the correlation step. The claims contemplate that reports are *integrated* simply by virtue of the fact that they are reports, while reports are *correlated* on the basis of other, shared commonalities. By requiring the same level of data processing in both the integration and correlation steps, the Defendants essentially equate the two steps, whereas the claims themselves show that those steps are different.

The Defendants' arguments against SRI's construction of "correlating" similarly misapprehend the law relevant to construction of dependent claims. The Defendants fault

SRI for not specifying that "correlating" requires that reports be combined "into another functional unit." But, as discussed above, the limitations of the independent "integrating" claims are necessarily also limitations of the dependent "correlating" claims, and thus it is quite clear that, using SRI's proposed constructions, "correlating" requires that reports be combined into another functional unit. To restate that correlating, like integrating, requires a new functional unit would simply make the construction redundant.

B. Statistical Detection And Statistical Profile Limitations

1. Building at least one long-term and at least one short-term statistical profile from at least one measure of network packets

Claim Term	**"building at least one long-term and at least one short-term statistical profile from at least one measure of the network packets"**
SRI Construction	creating at least one statistical description representative of historical network activity, and creating at least one statistical description of recent network activity, where the descriptions are based on one or more measures of network packets

Claim Term	**"building at least one long-term . . . statistical profile from at least one measure"**
Defendants' Joint Construction	automatically generating and updating an exponentially aged probability distribution of historically observed activities

Claim Term	**"building . . . at least one short-term statistical profile from at least one measure"**
Defendants' Joint Construction	automatically generating and updating an exponentially aged probability distribution of recently observed activities

Rather than jointly embracing a construction previously proposed by either ISS or Symantec, the Defendants here propose a new variation. Of the many possible limitations described in the specification with respect to statistical profiles, the Defendants select three limitations for inclusion in their proposed claim construction. This constant evolution and selectivity shows their results-oriented approach to claim construction, and provokes the following question: Is there any reason, aside from

creating a non-infringement position, for requiring that statistical profiles be construed as having the three specific features, and only those, the Defendants now propose?

Specifically, the Defendants propose that statistical profiles be 1) "generat[ed] *and* updat[ed];" 2) "exponentially aged;" and 3) "probability distribution[s]." As an initial matter, none of these limitations appears in the claims; they are instead imported from a preferred embodiment, and thus should be rejected. Aside from this fundamental problem, the Defendants provide no justification for so limiting the claims.

As to the first limitation, the Defendants provide no reason whatsoever to construe "building" to mean "generating and updating."

As to the second limitation, even to the extent that the specification describes a short-term profile that is exponentially aged, that description is not always applied and is never expressly applied to a long-term profile. The Defendants' contention that the only described difference between short-term and long-term profiles is recency of observed activity is contradicted by the same text that they cite from the specification: "[t]he short-term profile accumulates values between updates, and exponentially ages," [Ex. A at 6:41-42], but "[t]he long-term profile is itself slowly aged to adapt to changes in subject activity." [Ex. A at 6:51-53]. Thus, neither the claims nor the specification require both profiles to be exponentially aged, and accordingly the Defendants' proposed construction must be rejected.

As to the alleged limitation requiring that statistical profiles be probability distributions, this limitation is nowhere found in the claims themselves. The Defendants again import this limitation from the specification, even though the statistical profiles are never even described in the specification as "probability distributions." Moreover, the citations the Defendants rely on from the specification do not support their argument in any event, as they are clearly exemplary. [*See* Ex. A at 5:36-38 ("The profile engine *can* use a *wide variety* of multivariate statistical measures…"); 5:59-61 ("the profiler engine *can* build empirical distributions"); 6:8-10 ("multi-modal distributions *are*

accommodated"); 6:54-57 ("multi-modal and categorical distributions *are accommodated*.")]. Knowing the specification is inconsistent with their position, the Defendants rely almost entirely on extrinsic evidence from one of their experts, Dr. Staniford,[17] and citations from documents incorporated by reference — which the specification also expressly says are examples that "may" be used. [*See* Ex. A at 5:42-47 ("The profile engine *may* use a statistical analysis technique…")]. Because there is nothing in the claim language that supports the Defendants' proposal and the specification both expressly describes the profiles as "descriptions" and states that the various descriptions are examples that *may* or *can* be used, the Court should reject the Defendants' attempt to limit the claimed profiles to "probability distributions."[18]

Finally, the Defendants disparage SRI for 1) failing to specify that statistical profiles are built automatically; 2) construing "statistical profile" to mean "statistical description;" and 3) allegedly failing to account for a description of statistical profiles found in the specification. As to the first point, SRI does not dispute that statistical profiles are built automatically; that is readily apparent from the whole context of the claimed inventions and the recitation of "building" in the claims. As to the second point, the Defendants' criticism is disingenuous given that ISS had also proposed that "profile" be construed to mean "description," and abandoned that construction only recently upon the filing of the Joint Brief. Moreover, SRI's language is intended to explain the claimed terminology and is consistent with the specification, which describes the system maintaining and updating "a description of behavior with respect to these measure types in an updated profile." [Ex. A at 6:38-39]. As to the third point, the failure of SRI's

---

[17] The example relied upon by Dr. Staniford, regarding failed login attempts, is directly contrary to the discussion in the specification which actually describes failed logins (themselves inherently suspicious) as being analyzed with signature methods rather than statistical measures.

[18] Again, the Defendants' construction creates confusion and ambiguity rather than clarifying the claims because it introduces the undefined terminology "exponentially aged probability distribution" as a substitute for "statistical profile."

proposed construction to import limitations from the specification that are nowhere found in the claims is both intentional and in keeping with well-established principles of claim construction mandated by Federal Circuit case law.

2. Determining whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity

Claim Term	**"determining whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity"**
SRI Construction	SRI does not believe the term needs construction but, if construed, should be construed to mean using the result of the comparison to decide whether the monitored activity is suspicious
Defendants' Joint Construction	determining whether the difference between the short-term statistical profile and the long-term statistical profile exceeds a threshold that is empirically determined to indicate suspicious activity based on the historically adaptive deviation between the two profiles, requiring no prior knowledge of suspicious activity

While SRI does not believe that this claim phrase requires construction because its meaning within the context of the claims is evident, the Defendants contend that this already lengthy claim language should be "clarified" for the jury by replacing the last four words — "indicates suspicious network activity" — with twenty-nine new words. The Defendants' prolix construction in fact obfuscates rather than clarifies the meaning of this phrase by introducing additional language, such as "historically adaptive deviation," that is far more vague than the language the Defendants contend requires clarification. For that reason alone, but not only for that reason, the Defendants' proposed construction should be rejected.

The Defendants' proposed construction does not interpret the claim language in any way — instead, it merely attempts to import limitations that are simply not present in the claims. This is immediately evident from a comparison of the actual claim language (in black) and the proposed additional limitations (in red):

> **determining whether the difference between the short-term statistical profile and long-term statistical profile exceeds a threshold that is empirically determined to indicate~~[s]~~ suspicious ~~network~~ activity based on the historically adaptive deviation between the two profiles, requiring no prior knowledge of suspicious activity**

The actual claim language is merely reiterated, and limiting language is inserted. The proposed construction, at best, fails to define or clarify anything; at worst, it is a transparent attempt to import a limitation (the use of a specific kind of threshold) that is nowhere found in the claims. The Defendants' proposed construction should be rejected. Construing the term to require a threshold of any type would be an improper importation of limitations from a preferred embodiment. *Phillips*, 415 F.3d at 1316. Construing it, as the Defendants do, to require importation of a specific type of threshold is even more egregious. The Defendants' construction should be rejected.

The Defendants disparage SRI's construction for allegedly encompassing improper types of "threshold" analysis. As discussed above, the claims do not require, or even mention, the use of thresholds, and accordingly the Defendants' criticism is unfounded. The Defendants also mischaracterize the specification as teaching that the claimed statistical detection step cannot use fixed threshold values reflecting prior knowledge of suspicious activity. The cited text of the specification states that "a monitor ***can*** distinguish between normal error levels . . . without . . . setting an unvarying threshold." [Ex. A at 13:22-37 (emphasis added)]. This is described as a possibility, not a requirement. Likewise, that a determination of suspicious activity "require[s] no a priori knowledge of intrusive or exceptional activity" [Ex. A at 6:57-58] obviously does not mean that a determination can only be made in the absence of prior knowledge. The Defendants' proposed limitations are features of a preferred embodiment that are not found in or required by the plain language of the claims. Accordingly, the Defendants' construction should be rejected and SRI's construction should be adopted.

3. Statistical Detection Method

Claim Term	**"a statistical detection method"**
SRI Construction	SRI does not believe the term needs construction but, if construed, should be construed to mean a method of detecting suspicious network activity by applying one or more statistical functions in the analysis of network traffic data
Defendants' Joint Construction	A method of detecting suspicious network activity which comprises building a *long-term statistical profile* and a *short-term statistical profile*. This method requires no prior knowledge of suspicious network activity. This method is not a signature matching detection method or threshold analysis

SRI does not believe that the terms "statistical detection method" requires construction, as it has a plain English-language meaning that is readily understood. *Johnson Worldwide Assocs. v. Zebco Corp.*, 175 F.3d 985, 989 (Fed. Cir. 1999). The Defendants contend that jurors will better be able to understand this simple three-word phrase if it is construed to have a *forty-three* word meaning. Even assuming that clarity can be achieved through an order-of-magnitude increase in complexity, the Defendants' construction should be rejected for other reasons.

First, the Defendants improperly import limitations which they admit are found only in the preferred embodiment and not in the claims themselves, completely ignoring that the only limitation on "statistical detection" found in the claims is that it be performed by a network monitor. Hinting again at an issue of enablement, the Defendants argue that statistical methods were not known in the art in November 1998, and thus that the term "statistical detection method" must be limited to the preferred embodiment, because no other construction would allegedly have been enabled.

The Federal Circuit has "expressly rejected the contention that if a patent describes only a single embodiment, the claims of the patent must be construed as being limited to that embodiment." *Phillips*, 415 F.3d at 1323. The reason for this is "because persons of ordinary skill in the art rarely would confine their definitions of terms to the exact representations depicted in the embodiments." *Id.* The Defendants attempt to

avoid the controlling precedent that explicitly rejects their proposed construction by suggesting that no other method was known to those having ordinary skill in the art in 1998. But the Defendants' characterization of what was known in the art in 1998 is incorrect. Indeed, the very prior art that the Defendants allege anticipated the patents-in-suit demonstrates that persons of skill in the art knew what a statistical detection method was in the relevant timeframe, although such methods were not applied in the context of a hierarchical analysis system as recited in the asserted claims of the '212 patent. [*See, e.g.*, Ex. F (NIDES Report); Ex. G (JI-NAO Report)]. Tellingly, none of the Defendants' experts opined that the specification of the patents-in-suit lacks an enabling disclosure of a statistical detection method.

The construction that the Defendants propose is also improper under the doctrine of claim differentiation. It is well-established that a construction that narrows a claim term in a manner that is explicitly accomplished by limitations that appear in dependent claims is presumptively unreasonable and wrong. *TurboCare Div. of Demag Delaval Turbomachinery Corp. v. General Electric Co.*, 264 F.3d 1111, 1123 (Fed. Cir. 2001). *See also Phillips*, 415 F.3d at 1315 ("[T]he presence of a dependent claim that adds a particular limitation gives rise to a presumption that the limitation in question is not present in the independent claim."). While the Defendants insist that proper construction requires the limitation that "this method is not a signature matching detection method", they also concede that "the claims distinguish between statistical detection methods and signature detection methods."[19] Because the claims themselves provide the distinction that the Defendants propose, their construction is unnecessary, and must be rejected.

While the Defendants acknowledge that the patent claims distinguish between statistical and signature detection methods, they fail to acknowledge that the claims also distinguish between "statistical detection methods" and the use of "statistical profiles."

[19] Joint Brief at 37.

For example, the '212 patent claims the use of a statistical detection method, but not the use of long-term or short-term statistical profiles, while the '338 patent more specifically claims the use of long-term and short-term statistical profiles. The Defendants propose a construction under which statistical detection method, by definition, requires the use of long-term and short-term statistical profiles. That construction would render the distinction between what is claimed in the '212 patent and what is claimed in the '338 patent meaningless. Again, because the distinction that the Defendants propose is achieved through claim differentiation, their construction is presumptively wrong, and must be rejected. *Phillips*, 415 F.3d at 1315; *TurboCare*, 264 F.3d at 1123.

The most pernicious aspect of the proposed construction, and the one Symantec attempts to leverage into summary judgment of non-infringement, is the "or threshold analysis" tagged to the end of the negative limitation provided.[20] But, as discussed above and explained in SRI's Opening Brief, this argument is inconsistent with the Defendants' own description of the statistical analysis method of the '338 patent as involving use of a threshold. Accordingly, even the Defendants recognize that "thresholds" can play a part in a statistical detection method, as well as a signature-based method, and the mere existence of a threshold is not determinative of whether one is using a statistical detection method or not. The Defendants simply cannot leverage the patents' classification of the example "threshold analyses" described as "rudimentary, inexpensive signature analysis" into the conclusion that any use of any type of threshold must therefore be classified as a "signature" rather than a "statistical" method. A use of a threshold could be "statistical" if that threshold is itself determined by statistical methods (*e.g.*, a historically adapted threshold) or if a fixed, predetermined threshold is applied to some statistically derived data set (*e.g.*, comparing the ratio of SYN requests to the total of SYN_ACK and ICMP messages to a threshold to determine if there is an "imbalance"). [*See* Ex. A at 6:65-67;

[20] *See, also*, the related discussion in SRI's Response to Symantec's Motion for Summary Judgment for Non-Infringement at 3 to 7.

13:37-43]. Thus, the Defendants' attempt to limit "statistical detection method" to require statistical profiles or to exclude any use of "thresholds" whatsoever should be rejected.

C. Signature Matching Detection Method and API

1. Signature Matching Detection Method

The Defendants appear to have abandoned their effort to have this claim phrase construed. Why? Because their proposed definition, including the admission that signature matching is a "method of detecting suspicious network activity," is directly contrary to the opinion of ISS's expert, Mr. Smaha. He attempted to distinguish ISS's products from the claims as allegedly relying only on signature methods, which in Mr. Smaha's opinion detect only "**known** malicious" activity rather than "**suspicious**" activity [Ex. H (Rebuttal Expert Report of Stephen E. Smaha at 6, 8]. The Defendants' own original construction recognizes that Mr. Smaha's opinion is contrary to the patents.

This conflict may also be the reason the Defendants appear to have abandoned their effort to construe "signature matching detection methods" as equivalent to "threshold analysis", preferring now instead to try to win the day through a negative limitation of "statistical detection." For the same reasons (described above) that using thresholds is not necessarily excluded by the phrase "statistical detection methods," use of thresholds cannot necessarily be equated with signature matching. The use of a threshold alone is simply not determinative of whether a method is "statistical" or "signature-based." *See, e.g.*, Ex. I (Expert Report of Stuart Staniford) at 31 (emphasis added); Ex. J (Staniford Tr.) at 65:5 (explaining use of thresholds in statistical detection); Ex. K (Porras Tr.) at 339:25-340:23 (explaining that threshold comparison techniques may sometimes be considered as a form of signature analysis, and may in other circumstances be considered statistical analysis techniques) and Declaration of Dr.

George Kesidis In Support of SRI International, Inc.'s Responses To Defendants' Summary Judgment Motions at ¶¶ 16].

Given that the Defendants appear likely to continue to try and leverage an implicit construction of "signature matching detection method" into some contention as to non-infringement or invalidity, SRI asks the Court to adopt SRI's proposed construction of this phrase for the reasons set forth above and in SRI's Opening Brief.

2. API

It is not surprising that the Defendants did not address the API claim element in their Joint Brief because, as SRI explained, the construction of API was raised for the first time in the Defendants' expert reports as a newly alleged ground for non-infringement. In an effort to prevent the Defendants from creating a non-infringement issue through such a back-door construction, SRI addressed the claim element in its Opening Brief. For the reasons set forth in that brief, the Court should construe the claimed API to mean "a set of routines used to provide for communication of data between application programs or processes."

III. CONCLUSION

For the foregoing reasons, and as explained in SRI's other briefs and pleadings, SRI respectfully requests that the Court adopt its constructions for the terms of the patents-in-suit.

Dated: June 30, 2006

FISH & RICHARDSON P.C.

By: */s/ John F. Horvath*

John F. Horvath (#4557)
FISH & RICHARDSON P.C.
919 N. Market St., Ste. 1100
P.O. Box 1114
Wilmington, DE 19889-1114
Telephone: (302) 652-5070
Facsimile: (302) 652-0607

Howard G. Pollack (CA Bar No. 162897)
Katherine D. Prescott (CA Bar No. 215496)
FISH & RICHARDSON P.C.
500 Arguello St., Ste. 500
Redwood City, CA 94063
Telephone: (650) 839-5070
Facsimile: (650) 839-5071

Attorneys for Plaintiff/Counterclaim Defendant
SRI INTERNATIONAL, INC.

50357727a.doc

CERTIFICATE OF SERVICE

I hereby certify that on this 30th day of June, 2006, I electronically filed **SRI'S RESPONSE TO JOINT OPENING CLAIM CONSTRUCTION BRIEF OF ISS AND SYMANTEC** using CM/ECF which will send notification of such filing to the following. A copy was also sent via hand delivery:

Richard L. Horwitz David E. Moore Potter Anderson & Corroon LLP Hercules Plaza 1313 North Market Street, 6th Floor P.O. Box 951 Wilmington, DE 19899 Telephone: 302-984-6000 Facsimile: 302-658-1192 Email: rhorwitz@potteranderson.com Email: dmoore@potteranderson.com	Attorneys for Defendant/Counterclaim Plaintiffs Internet Security Systems, Inc., a Delaware corporation, and Internet Security Systems, Inc., a Georgia corporation
Richard K. Herrmann Morris James Hitchens & Williams LLP 222 Delaware Avenue, 10th Floor P.O. Box 2306 Wilmington, DE 19899-2306 Telephone: 302-888-6800 Facsimile: 302-571-1750 Email: rherrmann@morrisjames.com	Attorneys for Defendant/Counterclaim Plaintiff Symantec Corporation

I also certify that on June 30, 2006, I mailed by United States Postal Service and by electronic mail, the above document(s) to the following non-registered participants:

Holmes J. Hawkins, III
Natasha H. Moffitt
King & Spalding LLP
1180 Peachtree Street
Atlanta, GA 30309
Telephone: 404-572-4600
Facsimile: 404-572-5145
Email: hhawkins@kslaw.com
Email: nmoffitt@kslaw.com

Attorneys for Defendant/Counterclaim Plaintiffs Internet Security Systems, Inc., a Delaware corporation, and Internet Security Systems, Inc., a Georgia corporation

Theresa A. Moehlman
Bhavana Joneja
King & Spalding LLP
1185 Avenue of the Americas
New York, NY 10036
Telephone: 212-556-2100
Facsimile: 212-556-2222
Email: tmoehlman@kslaw.com
Email: bjoneja@kslaw.com

Attorneys for Defendant/Counterclaim Plaintiffs Internet Security Systems, Inc., a Delaware Corporation, and Internet Security Systems, Inc., a Georgia Corporation

Lloyd R. Day, Jr.
Robert M. Galvin
Paul S. Grewal
Day Casebeer Madrid & Batchelder, LLP
20300 Stevens Creek Boulevard, Suite 400
Cupertino, California 95014
Telephone: 408-873-0110
Facsimile: 408-873-0220
Email: pgrewal@daycasebeer.com

Attorneys for Defendant/Counterclaim Plaintiff Symantec Corporation

/s/ John F. Horvath
John F. Horvath